Spring 2016 Vol. 7 No. 1

MCU Journal

Published by Marine Corps University Press

Identity, Attribution, and the Challenge of Targeting in the Cyberdomain

Colonel Glenn Voelz, USA, and Sarah Soliman

Abstract. The cyberdomain has become "key terrain" of irregular warfare with state and nonstate actors leveraging social media and other digital tools for command and control, intelligence gathering, training, recruiting, and propaganda. Department of Defense cyberstrategy highlights the urgent need for improved cyber situational awareness to reduce anonymity in cyberspace. This requires new technologies, doctrine, and analytical approaches for identifying and targeting adversaries operating in a digital landscape. This article examines identity-based targeting approaches developed during recent conflicts as a possible starting point for this effort.

Keywords: Cyberdomain, social media, targeting, identity intelligence, attribution, gray zone conflicts, hybrid warfare, Islamic State, terrorism, biometrics, network analysis, big data, activity-based intelligence, high-value individuals

One of the early lessons learned during the conflicts in Iraq and Afghanistan was how legacy intelligence systems and methods designed for waging conventional warfare against state-based adversaries could not provide the kind of information needed to effectively target irregular combat-

Col Glenn Voelz, USA, is the senior intelligence analyst on the International Military Staff at NATO Headquarters. He was previously the U.S. Army War College fellow in the Massachusetts Institute of Technology's Security Studies Program and at MIT's Lincoln Laboratory. He is a graduate of West Point and holds advanced degrees from the University of Virginia and the National Intelligence University.

Sarah Soliman spent two years in Iraq and Afghanistan as a technician supporting Department of Defense biometrics, forensics, and sensitive site exploitation, including time with U.S. Special Operations Command. She now studies emerging technology trends as a project associate at Rand in Washington, DC, and is pursuing a PhD through King's College London Department of War Studies.

MCU Journal vol. 7, no. 1
Spring 2016
www.mcu.usmc.mil/mcu_press
DOI:10.21140/mcuj.2016070101

ants.[1] These new adversaries were organized as distributed networks comprised of individuals often indistinguishable from surrounding populations. This operational challenge demanded new technologies and methods for identifying individual combatants, characterizing and geo-locating their activities, and analyzing the structure of their networks. Within this operational environment, combatant identity and pattern of life information became crucial elements of high-value targeting and the process of removing insurgents and terrorist networks from the battlefield.[2]

In many respects, this mode of warfare marked a major paradigm shift for the U.S. military. It demanded intelligence collection technologies and analytical methods very different from those designed for detecting motorized rifle battalions and targeting conventional weapons platforms. These adaptations evolved over a decade of intense counterinsurgency and counterterrorism campaigns against irregular adversaries that transformed methods of operational targeting and made combatant identity into a highly salient feature of modern combat. The evolution of identity-based targeting involved a process of doctrinal and technical innovation that brought new tools to the battlefield, such as biometrics, forensics, and DNA analysis.[3] These capabilities helped U.S. forces navigate the complex human terrain of the irregular battlefield and "put a uniform on the enemy" by reducing their ability to use anonymity for military advantage.

These technologies were applied within the context of new doctrinal concepts, such as Identity Intelligence (I2) and Find, Fix, Finish, Exploit, Analyze, and Disseminate (F3EAD). In I2, various identity attributes (biologic, biographic, behavioral, and reputational information) were fused with other tactical information to connect individual combatants to other persons, places, events, and materials on the battlefield. The F3EAD cycle was enabled by data-intensive analytical methods deeply influenced by social network theory and targeting processes specifically designed for engaging high-value individuals and dismantling their networks.

The next evolution in warfare is likely to reflect elements of continuity with these recent experiences even as specific tools and methods evolve. Future adversaries will continue to seek out asymmetric means to circumvent U.S. conventional force advantages. To do this, they will most certainly exploit cutting-edge commercial technologies and communications to generate tactical leverage against well-equipped militaries. As in recent conflicts, these adversaries are likely to avoid direct engagement by using anonymity to conceal operations, protect networks, and complicate targeting for U.S forces. Some of these methods resemble what commentators have dubbed "gray zone" conflicts, or wars characterized by " 'hybrid' threats that may combine subversion, destabilizing social media influence, disruptive cyber attacks, and anonymous 'little green men' instead of recognizable armed forces making overt violations of international borders."[4]

Moreover, these methods are likely to be adopted by state as well as nonstate actors. As General Joseph L. "Joe" Votel, commander of U.S. Special Operations Command, recently noted, such conflicts are likely to be defined by ambiguity and even uncertainty regarding the parties involved.[5]

Within this operational paradigm, the cyberdomain is likely to emerge as "key terrain" of these future battlefields.[6] Over the last few years, a range of nation-state and nonstate actors from Russia to the Islamic State have aggressively leveraged cybertools as part of their intelligence gathering, operational planning, internal communications, recruiting, and strategic messaging—all directed toward creating tangible effects in the physical battlespace. As such methods expand, they are likely to present conventional military forces with targeting challenges similar to those experienced during the last decade in Iraq and Afghanistan. Specifically, modern irregular adversaries have been empowered by their ability to hide among the populace, avoid attribution, and complicate the targeting process for conventional military forces.[7] These methods apply to the cyberdomain as well as the physical battlespace. Adversaries are already leveraging cybertools to create demonstrable effects in the physical landscape while manipulating their digital identities to hide, deceive, and confuse observers as to the nature of their activities. Furthermore, the technical tools and methods for masking identity and obscuring attribution are increasingly available even to those with limited technical expertise.

One U.S. Department of Defense (DOD) cyberspace policy report observed how the technical protocols of the Internet provide the means of protecting anonymity and veiling attribution in a manner that "both nations and non-state actors clearly understand."[8] Such methods are likely to be used in the future as a means for generating strategic advantage. Yet even as U.S. forces increasingly maneuver within this digital landscape, they lack sufficient situational awareness concerning the other actors seeking to influence the operational environment. This situation presents a growing risk for conventional military forces, particularly at the operational level where units lack the robust capabilities to identify, monitor, and target key actors in the cyberpersona layer.[9] Problems include a lack of technical tools and expertise enabling commanders to visualize the cyberpersona layer (see figure 1) as well as a doctrinal framework for assessing risks and making effective targeting determinations within this environment.

Adapting to these new challenges will likely require a paradigm shift equal in scope and complexity to the recent evolution of identity-based targeting. In fact, this example may offer several useful parallels in this process, including a template for the process of military innovation and the development of technical tools and supporting doctrine to enable military forces to operate against these new threats. Similar to the complex human terrain of Iraq and Afghanistan, the cyberdomain represents an ill-defined and unbounded battlespace. It contains

adversaries who may not wear uniforms or even occupy a discrete physical area on the battlefield. These virtual combatants are likely to have the technical means to conceal identities, veil attribution, and mask movements across the digital landscape. Within this environment, the issue of combatant identity is likely to persist as one of the most challenging aspects of effective targeting.

Given these concerns, it may be shortsighted to simply view cyberthreats in a narrow technical sense by limiting them to data packets and malware. As this article suggests, there are several important parallels between the identity-based targeting methods applied in the physical domain and what will be needed for military forces to effectively target future adversaries in the cyberdomain. A key aspect for consideration involves developing new methods that link abstract cyberpersonae to actual physical identities, which reveal the nature of individuals' networks, methods, objectives, and functions. As one group of experts recently observed, even in the highly technical and abstract domain of cyberspace, "all operations still begin with a human being."[10]

Anonymity and Power in the Cyberdomain

The dramatic rise of the Islamic State in Iraq and the Levant (ISIL) perhaps offers the most vivid example of how the cyberdomain has become a highly relevant aspect of the contemporary operational environment. Over a relatively short period, ISIL has demonstrated how a combination of digital technologies, global communications networks, and social media platforms can be combined to generate powerful effects in the physical battlespace. The group has made extremely effective use of these tools for operational planning, disseminating training materials and technical information, and coordinating among widely dispersed affiliates and supporters. ISIL famously proliferates high-quality media content across multiple platforms as part of its strategic messaging and recruiting campaigns.[11] Its social media presence and distribution of digital magazines, such as *Dabiq* and *Konstantiniyye*, provide dramatic examples of how terrorist organizations are now using cyberspace to amplify the power of propaganda and extend their influence. ISIL has even developed original web applications providing its supporters with direct access to video and text updates about life under the Islamic State and announcements of battlefield victories.[12]

Social media in particular has become a key enabler for insurgent groups and terrorist organizations in recent years. Popular applications like Twitter, YouTube, Facebook, Tumblr, and Instagram have created a digital ecosystem providing such nonstate actors with unprecedented global reach. Militant groups in Gaza, terrorist cells in Mali, oil traffickers in Nigeria, and pirates off the Somali coast have all used social media as ad hoc communication networks and as platforms for conducting information operations. In many respects, social media provides the ideal medium for adversaries who operate as highly distributed entities but

lack the technical capabilities and financial resources to build and manage formal command and control networks. The recent National Intelligence Council report, *Global Trends 2030*, noted how these social media architectures have become "inherently resistant to centralized oversight and control," enabling individuals, small groups, and ad hoc coalitions of nonstate actors to shift traditional power sources and authorities.[13]

The Syrian conflict provides perhaps the most powerful example of how the cyberdomain has become fully interwoven into the fabric of modern conflict. This war has been called "the most socially mediated civil conflict in history," with fighters routinely using Facebook, YouTube, Twitter, Diaspora, and Snapchat for a variety of operational, communication, and propaganda functions.[14] Analysis from late 2014 identified at least 46,000 Twitter accounts used by members and supporters of the Islamic State while the Federal Bureau of Investigation (FBI) estimated that some 200,000 people each day access the group's messaging via social media to include "videos, instruction manuals, and other material posted on militant Islamist social media sites."[15] While ISIL has perhaps become the most adept user of such tools, the phenomenon is by no means limited to the Islamic State. In Syria, the al-Qaeda linked al-Nusra Front has also used social media for posting press releases and issuing informal communiqués including text, photographs, and videos detailing recent fighting, even posting personalized eulogies for its members killed in combat.[16] Al-Qaeda is often credited with establishing the early model for Internet-based jihadist propaganda with the publication of its online magazine *Inspire*, designed for outreach to English-speaking Muslims. More recently the group has launched a new branch focused on cyberoffensive operations, allegedly executing a campaign of digital defacements, data exfiltrations, and denial of service attacks against Western interests.[17]

Cyberplatforms have also been used extensively for dissemination of operational information, recruiting, and training purposes.[18] For example, hundreds of websites and online forums host information on the use of explosives, fighting techniques, and links to encryption programs designed to help followers protect their sensitive communications. The director of Great Britain's National Security Agency counterpart, Government Communications Headquarters, recently described Twitter, Facebook, and WhatsApp as the "command-and-control networks of choice for terrorist and criminals."[19]

One important characteristic distinguishing the cyberdomain from a conventional physical battlespace is the variety of means for adversaries to anonymize their activities. This issue represents a significant dilemma for military commanders who increasingly are unable to identify actors seeking to exert influence within a given area of operations, whether they are nation-states, foreign intelligence services, hackers, criminals, or terrorists. From a targeting perspective, the primary challenge is linking the cyberpersona to an actual identity behind the digital repre-

sentation. As one cryptographer and security expert recently noted, "We're living in a world where we can't easily tell the difference between a couple of guys in a basement apartment and the North Korean government."[20] This phenomenon has led to a virtual "arms race between attackers and those that want to identify them."[21] One recent report has suggested that approximately 90 percent of terrorist activities taking place online now use social media as a networking tool for their operations, a situation that has created "a virtual firewall to help safeguard the identities of those who participate."[22]

These adversaries are actively exploiting technologies designed to conceal identity and veil attribution for operations conducted in the cyberdomain. Online jihadist forums routinely advise participants on how to avoid detection when web browsing, including steps for removing geo-location and metadata from cell phone images and social media content.[23] ISIL in particular has been adept at modifying its cyberbehavioral profiles by changing computers, cell phones, and messaging apps after one becomes compromised.[24] Some ISIL members are reportedly moving to more secure private messaging apps, such as Telegram, Kik, and WhatsApp, as a means of protecting internal communications.[25] These methods include the use of encryption and data-destroying software designed to frustrate surveillance methods.[26] FBI Director James B. Comey has been outspoken over his concerns that adversaries are increasingly "going dark" by employing tools that make it difficult for legitimate authorities to identify and track emerging threats. This issue, however, has been controversial and opened a vigorous debate among security experts and privacy advocates on the emerging challenges of encryption.

Shortly after ISIL's November 2015 attacks in Paris, the group announced that it would move some of its propaganda materials to the so-called Dark Web as a means of thwarting efforts by social media firms to identify and remove extremist content from their sites.[27] ISIL and other groups have already made use of such tools as the Onion Router (Tor) that enable users to communicate, post, and view online content anonymously.[28] While not offering perfect protection, Tor and similar technologies help mask IP addresses and server locations while encrypting data packets and routing messages through multiple nodes, which make it difficult for authorities to track and identify users. These anonymity-granting systems form the architecture for a sizable portion of Internet traffic that is virtually inaccessible by means of standard web browsers. Tor and other anonymizing software evolved as classic dual-use technologies with many legitimate uses; however, they have also created a virtual safe haven for illicit activities.[29] More recently there has been suggestion that these tools have become shadow command and control networks for terrorist recruitment, financing, and planning.

In addition to the Dark Web, the evolution of digital cryptocurrencies, such as Bitcoin, provide another means for conducting pseudonymous transactions that

are difficult for authorities to monitor and trace.[30] For example, Bitcoin is considered pseudonymous because an individual user is represented by a random, cryptographically generated string of digits that do not directly reveal a participant's identity. These architectures generally enable users to transfer funds with lower risk of detection and greater ability to conceal their physical location.[31] There is also evidence that some terrorist groups are using digital currencies to finance activities, a trend that is likely to be a growing concern as Western governments close off terrorist access to the legitimate international financial system.[32] The head of the U.S. Treasury Department's Financial Crimes Enforcement Network recently cited the growing risk from global point-to-point transactions and digital pseudonymity that enables these groups to move funds instantly across borders, often without detection.[33] Highlighting these concerns, National Security Agency Director Admiral Michael S. Rogers recently revealed the increasing amount of time his agency spends monitoring threats on the Dark Web and tracking people who cannot easily be found through conventional digital surveillance methods.[34]

Protected identities and complicated attribution have also made the cyberdomain an ideal space for conducting digital "denial and deception" operations. Denial and deception describes actions taken by an adversary to degrade or neutralize an opponent's intelligence collection or efforts that deliberately mislead observers as to the true nature of an activity. Cyberspace offers many tools and methods for crafting such misperception. The Internet is rife with fake Twitter accounts, digital avatars, and anonymizing software that can be used toward such ends. One such example was observed in early 2015 when a group known as the Cyber Caliphate, originally believed to be affiliated with ISIL, gained notoriety by briefly taking control of U.S. Central Command's Twitter account and exposing the personal information of some senior U.S. military members. Several months later, however, a private cyberintelligence firm called into question the group's ISIL affiliation and revealed possible links to a Russian-backed cyberespionage group that had been associated with previous attacks against "NATO, the Ukrainian government, and European Union networks."[35] These connections became evident only after a thorough forensic analysis revealed technical indications of a digital false flag operation used as a deliberate attempt to conceal the source of the attacks.[36]

Another example of spoofed digital identities used for military purposes was seen recently when a pro-Syrian regime group known as the Syrian Electronic Army (SEA) created fake online avatars to identify and target opposition members.[37] In this example, fictitious personae were used as part of a phishing campaign to gather detailed personal information including names, locations, and IP addresses of opposition members, media activists, humanitarian aid workers, and other individuals deemed dangerous to the regime.[38] From this information, SEA was able to access users' Skype accounts, mobile apps, and social media sites to

exploit address books, SMS messages, and email contacts from their targets. This kind of aggressive social media exploitation produced what was described as "actionable military intelligence for an immediate battlefield advantage" that enabled pro-Assad forces to identify, track, and target key opposition members.[39] SEA in effect operated as a de facto national cyberforce conducting cyberoperations on behalf of the regime; however, the identities of the individuals behind these operations and the nature of their relationship to the government remain ambiguous.[40] According to experts in the field, such methods are predicted to become "a routine part of even the most low-tech, if brutal, civil wars and available to those operating on a shoestring budget."[41]

All of these examples demonstrate the degree to which use of the cyberdomain by irregular adversaries has altered the relative balance of power vis-à-vis conventional military forces. The first digital revolution—based on advances in data processing, remote sensing, and satellite communications—was instrumental for enabling well-resourced state militaries to operate on a global scale, share real-time information, and concentrate combat power across time and space. Due to the complexity and expense of these systems, the operational benefits of this first revolution were generally limited to a handful of large military forces; however, the democratization of digital technologies has arguably overturned this dynamic.

Social networking, mobile communications, and global access to the Internet have enhanced the power of individuals and small groups relative to that of nation-states and hierarchical bureaucratic entities. The second digital revolution has lowered the barrier of access to advanced technical capabilities previously limited to first tier militaries. Now, relatively sophisticated cybertools are available even to poorly resourced actors. This rapid diffusion of digital technology has arguably become a key enabler for irregular warfare and accelerated the disaggregation of power away from conventional military forces.[42] The cyberdomain provides nonstate groups with a means to communicate, coordinate, and project influence on a global scale without requiring significant investment in research and development infrastructure or even a formalized program of procurement. These developments present a number of operational challenges for U.S. forces as well as questions on how to properly place these emerging threats within an appropriate doctrinal framework.

An Evolving Doctrinal Framework for Targeting in the Cyberdomain

The aforementioned examples of how ISIL and other nonstate actors are using the cybertools to create effects in the physical battlespace presents a number of challenging doctrinal questions. Technically speaking, most of these activities do not constitute cyberoperations per se, even as adversaries use cybertools to

produce demonstrable effects on the ground. The purposes of these activities—command and control, intelligence gathering, training, recruiting and propaganda—do not in fact represent cyberoperations in a doctrinal sense.[43] Nevertheless, they do exploit some of the unique characteristics of the cyberdomain to protect identity, veil attribution, and complicate targeting. The U.S. military has only recently begun considering the implications of how emerging cybertools may be applied on future battlefields as well as how to categorize such activities to develop appropriate responses, protocols, and targeting methodologies.

One expert in the field recently noted how the lack of historical example and the cross-domain nature of cyber makes it extremely difficult to fit these concepts into an existing doctrinal framework.[44] One important catalyst for these discussions was the 2011 publication of the *Department of Defense Strategy for Operating in Cyberspace*. This document marked a doctrinal paradigm shift by designating cyberspace as a distinct yet interdependent operational domain equivalent to that of air, land, maritime, and space.[45] This designation tacitly acknowledged the militarization of cyberspace and highlighted the fact that cyberoperations are expected to play a critical role in future conflicts.[46]

The DOD strategy paper also acknowledged the unique characteristics of cyberoperations that complicate the direct application of conventional warfighting concepts to this domain. Most obviously, threats in cyberspace do not recognize national boundaries or formally declared zones of conflict. They are ill defined, asymmetric, and often difficult to attribute.[47] They do not always have a discernable kinetic parallel in terms of generating unambiguous physical effects. Furthermore the nature of the technical tools used in this domain can make it difficult to draw clear operational distinctions between cyberwar, cyberterrorism, cyberespionage, and cybercrime. These characteristics impose certain limitations on the application of state-centric security concepts such as deterrence, escalation, and proportionality in the development of military cyberstrategy.[48] Nevertheless, when it comes to targeting in the cyberdomain, existing doctrine still generally applies a conceptual framework that more or less mirrors the methods applied to conventional maneuver warfare.[49] This fact seems to reflect a degree of doctrinal inertia that dangerously underestimates the unique operational characteristics of this domain.

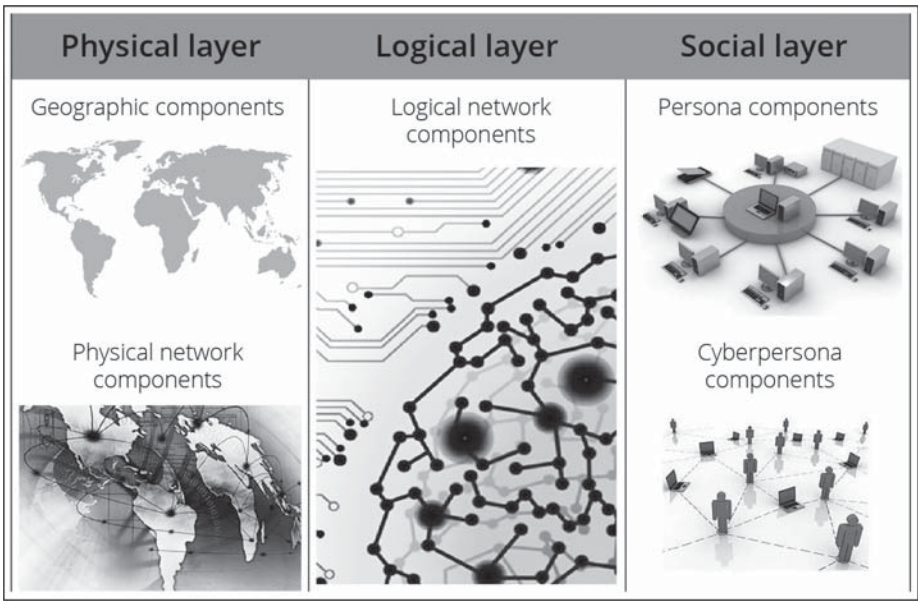
As already discussed, one of the most important characteristics making the cyberdomain uniquely challenging from a targeting perspective is the issue of attribution. As a basic technical matter, this differs significantly from conventional military operations where uniforms, weapons systems, and physical geography generally produce detectable signatures that can reveal an adversary's identity, location, and activities.[50] The conventional Intelligence, Surveillance, and Reconnaissance capabilities at the operational level, however, presently offer relatively few tools to help commanders visualize the cyberpersona layer

of their immediate operational environment.[51] At these echelons, cyberintelligence focused primarily on issues of network defense and information assurance. This situation is partly due to a lack of cyber-resources and technical expertise below the strategic level; however, there is also a conceptual component that has slowed progress on this front.

U.S. military organizations generally remain focused on conventional warfighting concepts and consequently struggle with the more abstract implications of how adversaries might apply cybertools to create effects in the physical battlespace. This mindset also applies generally to operational planners who are more comfortable thinking in terms of the traditional elements of combat power: mass, maneuver, and firepower. Yet, these factors are less obviously applicable as conceptual anchors for understanding the military effects of cybertools or selecting the best means of targeting adversaries operating within this domain.

Recent doctrinal publications have made some progress in offering a framework for understanding how the cyberdimension shapes the overall operational environment. *Cyberspace Operations* describes this space in terms of three distinct layers: a physical network forming the medium where data travels, a logical network representing the signal topology and arrangement of devices on the network, and finally the cyberpersona layer representing the digital representation of individuals or entities operating in cyberspace (figure 1).[52] The cyberpersona layer is the abstract representation of the actors behind the network and represents the most challenging aspect from a targeting perspective. For example, complex

Figure 1. The three layers of cyberspace



Adapted from U.S. Army, Cyberspace Operations Concept Capability Plan 2016–2028 *by MCUP.*

digital identities could manifest concurrently at multiple locations while some may not even be traceable to a single discrete physical node. A single entity may have multiple cyberpersonae, such as the case with Russian Internet trolls who conduct information campaigns by using dozens, sometimes hundreds of digital identities.[53] Alternatively, a single cyberpersona could represent numerous different user identities, such as the case with the online activist group Anonymous.[54] For this reason, the actions of a cyberpersona may not be easily be attributed to a state, an army, or an individual actor.

These abstractions make it difficult to conceptualize how military forces might effectively integrate cybereffects into a conventional targeting plan. Without a clearly defined adversary identifiable as a dot on a map, much of the basis for conventional targeting doctrine becomes untenable. Furthermore, in the cyberdomain, launching attacks against an adversary's computers, cell phones, and social media accounts may actually have the adverse effect of eliminating the only source of insight on the identities and operations of the network. In light of these challenges, the latest DOD cyberstrategy moves in the right direction by emphasizing the need for improved "intelligence and attribution capabilities help to unmask an actor's cyberpersona, identify the attack's point of origin, and determine tactics, techniques, and procedures" to support credible deterrence, response, and denial operations.[55]

One recent paper on cyberintelligence noted how dealing with these threats must go beyond the issue of network defense.[56] As doctrinally defined, cyberoperations do not encompass the growing scope of influencing activities that are now taking place in the digital domain. Therefore, cyberintelligence must evolve as an all-source discipline and not be limited only to the technical aspects of network protection. This means that cyberanalysts must also have an understanding of the human dimension of cyberoperations. This includes techniques for identifying the actors behind the keyboards; knowing how adversaries plan, coordinate, and execute their operations; and understanding what motivates them toward action.[57] In many respects, this makes targeting in the cyberdomain a logical extension of the identity-based approaches refined during recent conflicts.

New Technologies and Methods for Building Cyber Situational Awareness

As the cyberdomain increasingly represents "key terrain" of irregular warfare, the task of developing situational awareness will become a critical need for conventional military forces. This will involve integrating new technical tools and analytical methods designed specifically for identifying, tracking, and targeting anonymous actors using cybertools as a medium for creating effects in the physical landscape. The urgent need for "strong intelligence, forensics, and indications and warning capabilities to reduce anonymity in cyberspace and increase confi-

dence in attribution" was recognized in the DOD's most recent cyberstrategy document.[58] At the present time, however, military commanders, particularly at the operational level, still lack the technical means and analytical methods for identifying these actors, mapping their activities, and understanding how they exert influence on the battlefield. The high-profile case of Jihadi John demonstrated the power of being able to identify an unknown actor on social media and then link digital patterns of life information to an actual person, a physical location, specific activities, or associations; however, the hunt required national level assets far removed from operational commanders.[59]

Traditional computer network analysis can provide methods for obtaining some contextual information through technical means. For instance, an anonymous cyberpersona must still interface through a physical plane that contains information about device hardware and operating characteristics. Additionally, analysis of the logical plane may reveal such information as network addresses and configuration settings, and in some cases, even the geographic location of a user. While these attributes can help to characterize how a cyberpersona operates, they do not necessarily expose the identity of the individual behind the screen. To derive this type of information, a cyberpersona would need to be linked to an identifiable user account, digital certificates, or stored biometric data, but even this information may not provide a definitive picture of whose fingers are on the keyboard. This offers the cyberequivalent of signature-based targeting where analysts infer a target's identity based on the characteristics of observed activity. This method does not necessarily reveal exactly who is using a SIM card, however, only whether or not the users' activities fit a known behavioral pattern.

This example also highlights the point that insurgents, terrorists, and irregular combatants do not emanate the same technical signatures as conventional military forces, therefore characterizing and targeting these entities requires different collection methods and analytical approaches. This is true regardless of whether the adversary occupies a physical presence on the battlefield, hides among an indigenous population, or operates as a cyberpersona maneuvering through the digital landscape. Also, unlike professional armies that function on doctrinal precepts, irregular forces generally have less discernable templates guiding their actions, making predictive analysis a much more daunting challenge. For these reasons, identity-based targeting in the cyberdomain requires tools and methods that are better able to exploit remotely accessible attributes and indicators.

As one example, behavioral biometrics offers some potential techniques for establishing identity by indirect means that may be well suited to the challenges of cyberoperations. In general terms, behavioral biometrics refers to identifying characteristics that are learned or acquired over time rather than those based primarily on biology—for instance, using such features as "style, preference, knowledge, motor-skills or strategy" that people use in "human actions which result

from specific to everyday human skills."[60] Some common examples of measurable traits include handwriting, keystroke movements, or mouse dynamics. Other examples include distinguishing behavioral patterns that can be derived from common online activities, including email routines, digital device interactions, or credit card usage.

Where traditional biometrics can be limited in use, behavioral biometrics often provides missing benefits; most notable is behavioral biometrics' potential for "stand off" or noncompliant collection. For instance, patterns of email usage or web surfing offer the possibility of deriving unique user identifications with the advantage of nonobtrusive collection. Multiple studies have demonstrated how unique behavioral profiles can be derived from the peculiarities of message stylization, temporal activity, sentence structure, and other variables.[61] This has obvious applications for resolving ambiguous identities derived from user accounts or devices shared among multiple individuals. Similar applications have been developed to spot aberrant behavior on social media platforms, such as detecting fake Twitter and Facebook accounts. Behavioral biometrics can also be applied to help identify online deception campaigns by analyzing linguistic cues, usage patterns, social connections, and physical locations to help characterize the identities behind the posts.

Behavioral biometrics is also being used to modernize the analysis of "digital handwriting" or dynamic signatures derived from the unique way a user types or manipulate a digital device. These cognitive-biometric attributes are being used for identity authentication on mobile devices by analyzing such factors as handedness, hand tremor, eye-hand coordination, keystroke analysis, and other identifiable patterns derived from human–machine interactions.[62] Researchers have found these behavioral patterns to be "complex, nuanced and instinctive," thereby offering a highly accurate method for identifying individuals based on their use of digital devices.[63]

Another recent experiment has identified unique "egocentric video biometrics" derived from raw video footage taken from head- and body-mounted cameras.[64] One potential application of this technique would be the ability to locate all videos shot by a single user from within a large database of digital files even without the benefit of descriptive metadata. Similar techniques have been developed for generating biometric authentication from computer mouse manipulation and fitness tracking devices. Such information could be invaluable for identity verification when combined with precise geo-location derived from a mobile device or when correlated with other social media activity. As humans increasingly maintain nearly continual interaction with their digital devices, the field of behavioral biometrics potentially offers a range of techniques well suited for deriving identity information from online activities.

The ability to apply digital forensics or behavioral biometrics to positively

identify cyberpersonae will also increase the value of social media exploitation. While this remains a complex technical challenge due to vast amounts of low-value raw data, it does offer some means for mapping out an increasingly complex digital landscape and identifying key nodes of activity that could influence the physical battlespace. For example, in early 2014, analysts were able to track Russian military movement into Crimea using social media "bread crumbs" dropped by personnel preparing for mobilization. Separately, YouTube videos and Twitter messages posted by Russian irregulars provided the first hints of attribution for the downing of Malaysia Airlines Flight 17 in eastern Ukraine in July 2014.[65]

The ability to derive useful identity information of threat actors from a vast sea of digital activity will depend on major advances in computing power and new analytical methods. Artificial Intelligence, machine learning, and methods for dealing with the challenge of interpreting "big data" are areas where technology is expected to improve the ability of analysts to sort through large amounts of unstructured information to discern patterns, trends, and embedded associations among actors.[66] These tools could be particularly useful for discovering unseen correlations between the online activities of cyberpersonae and identity signatures in the physical domain. These tools have already demonstrated significant potential for improving the accuracy and power of standard biometric modalities, such as increasing the speed and accuracy of the image recognition applications used by Facebook, Google, Microsoft, and Twitter.[67]

In addition to new collection modalities, U.S. forces will need innovative approaches to informational management that are better suited for processing the vast amounts of data generated by a world of networked adversaries. A recent white paper by the under secretary of defense for intelligence highlighted the nature of this new environment by noting how individuals are increasingly becoming "self-documenting" by creating digital trails of potentially useful data during the conduct of their daily lives.[68] Ubiquitous interconnectivity via email, social media, digital commerce, and interface with the "internet of things" all combine to create a dense layer of interactions that expose much of who we are, where we go, and how we live our lives. This phenomenon presents a significant analytical challenge to derive meaning and actionable intelligence from the deluge of big data.[69]

Relatively new concepts—for example, Activity-Based Intelligence (ABI) and Object-Based Production (OBP)—provide some examples of analytical approaches that may be well suited for identity-based targeting in such data-rich environments. For example, ABI exploits the potential of big data by replacing collection discipline-centric analysis with an activity-based approach that focuses on all of the physical and virtual transactions associated with a specific entity.[70] ABI was originally conceived as an analytical approach optimized for identity-

based targeting on an irregular battlefield by focusing on the interactions and associations that define adversary networks.[71] This methodology was used to generate the kind of pattern of life analysis needed to dismantle insurgent groups in Iraq and Afghanistan.

Similarly, OBP is designed to deal with the challenge of information discovery and attribute correlation in an environment defined by disaggregated and heterogeneous data. As a method, OBP focuses on organizing information around a single object such as "people, places, and things [that become] the single point of convergence for all information and intelligence produced about a topic of interest."[72] This way of organizing data enables an analyst to visualize an entity's attributes, associations, and activities. For example, the information relating to an individual or group can be correlated with all information linked to that object, such as related attributes, common activities, or associations with other similar entities.[73] This could also include linkages to physical attributes from biometric, biographic, or forensic data. These novel approaches to information management may be better able to support the kind of data-intensive analyses that are needed to uncover deeply embedded associations from within large amounts of unstructured identity data scattered across the digital landscape.

As the military searches for new technologies to improve cyber situational awareness, it is likely that the commercial sector will provide some of the most powerful and innovative tools. As one example, the world of online advertising provides a useful model for how such cybercapabilities might evolve. In recent years, these firms have refined methods for resolving the identities of cyberpersonae using algorithms designed for probabilistic matching. Based on IP addresses, browser activity, authorship analysis, behavioral cues, and other digital signatures, these companies have been able to correlate identifiers so that entities can be tracked as they move across the cyberlandscape.[74]

Similarly, online retailers routinely gather detailed information about "spending habits, credit histories, web-surfing histories, social network postings, demographic information, and so on" for the purpose of market research and generating "precisely targeted advertising."[75] These activities can be linked and used to accurately track a single user across multiple devices and platforms by creating a "digital fingerprint" that correlates the cyberpersona to an actual physical identity. Social media companies are also becoming skilled at using geo-tracking, metadata, speech, and content analysis as methods for spotting unauthorized users or detecting fraudulent activities. In many ways, these examples offer precisely the kinds of tools needed by military cyberanalysts to help identify and analyze key influencers within an operational environment and potentially provide the kind of fidelity to target cyberpersonae across the digital landscape that the military has used to observe actors in the physical battlespace.

Conclusion

In recent years, there have been several vivid examples of adversaries using cybertools to create substantive military effects in the physical domain. These have included many activities falling outside of the strict doctrinal definition for cyberoperations. In particular, these tools have played an increasingly visible and consequential role in a wide range of irregular conflicts as part of terrorism activities and in gray zone or hybrid conflicts. One commonality among these examples is that both state and nonstate actors have leveraged the anonymity offered by cybertools as a means of creating strategic ambiguity and confusion over attribution of their activities. While deception and surprise have always been elements of warfare, these recent examples of state and nonstate actors using sophisticated technologies to mask identity present a significant challenge to conventional military targeting methods.

Dealing with this new kind of threat will require a paradigm shift in thinking about the meaning of situational awareness and targeting in the cyberdomain. A first important step will be better educating mid-level military leaders about the technical aspects of cyberoperations. This includes offering a clear doctrinal framework that integrates cyberconsiderations into the overall planning cycle and targeting process at the tactical and operational levels. This will require improved tools and analytical methods so that military commanders below that strategic level can have a common operational picture that takes into account all entities influencing the battlespace, including actors in the cyberpersona layer.

For the larger DOD enterprise, these solutions must also consider the looming challenge of encryption and other technical tools enabling adversaries to operate anonymously and avoid attribution. This problem will only become more acute as both state and nonstate adversaries continue to erode the slim relative advantages that the United States still enjoys with regard to cyberoperations—an edge that many experts suggest has already disappeared.

One starting point for designing a conceptual approach for cybertargeting may be to view it as a logical extension of the identity-based targeting techniques developed during recent campaigns. These examples share similarities in terms of the challenges faced by military forces when targeting irregular adversaries as well as the issues of identity and attribution in modern warfare. Expanding existing concepts such as I2 to the cyberdomain would provide a doctrinal framework for linking digital identities to corresponding biologic and biographic information in the physical domain. As a model for military innovation, the recent examples of biometrics and expeditionary forensics offer useful lessons learned for integrating nonmilitary technologies onto the battlefield and devising effective doctrinal frameworks for their use. These capabilities reflect an important operational need as adversaries increasingly use cybertools in order to create meaningful effects on the physical battlefield.

Notes

The views expressed in this article are the authors' own and do not reflect the official policy or position of the Department of Defense (DOD), the U.S. government, or NATO.

1. Among other studies, see Defense Science Board Task Force on Defense Intelligence, *Counterinsurgency (COIN) Intelligence, Surveillance, and Reconnaissance (ISR) Operations* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2011).
2. In the context of this discussion, the term *targeting* is applied in a broad doctrinal sense referring to "the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities." See U.S. Joint Chiefs of Staff (JCS), *Joint Targeting*, Joint Publication (JP) 3-60 (Washington, DC: JCS, 2013), vii.
3. The JCS defines biometrics as "the process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics." See JCS, *Joint Intelligence*, JP 2-0 (Washington, DC: JCS, 2013), GL-5. Intelligence information derived from biometric data helps link an unknown identity to places, activities, and networks and supports related pattern analysis to facilitate operations, such as high-value individual targeting. Forensics describes the scientific analysis of materials, such as DNA, used to link persons, places, things, and events.
4. David Barno and Nora Bensahel, "Fighting and Winning in the 'Gray Zone'," *War on the Rocks* (blog), 19 May 2015, http://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/. While there are multiple definitions of "hybrid conflict," the salient point for this discussion is the prevalence of irregular combatants using anonymity and ambiguous legal status for operational advantage. This may include a range of state, nonstate, and proxy actors whose uncertain identity and affiliation becomes a defining feature of the operational space. For a useful discussion on this topic, see Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Forces Quarterly*, no. 52 (1st Quarter 2009): 34–39, http://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-52.pdf.
5. Howard Altman, "'Gray Zone' Conflicts Far More Complex to Combat, Says Socom Chief Votel," *Tampa* (FL) *Tribune*, 28 November 2015, http://www.tbo.com/list/military-news/gray-zone-conflicts-far-more-complex-to-combat-says-socom-chief-votel-20151128/.
6. According to JCS, *Cyberspace Operations,* JP 3-12(R) (Washington, DC: JCS, 2013), GL-4, the term *cyberspace* refers to the "global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."
7. Attribution refers to the task of positively identifying threat actors and linking these entities to activities within the operational environment where JCS, *Information Operations,* JP 3-13 (Washington, DC: JCS, 2014), x, defines "operational environment" as a "composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander."
8. DOD, *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934* (Washington, DC: DOD, 2011), 4, https://fas.org/irp/eprint/dod-cyber.pdf.
9. "The cyber-persona layer consists of the people actually on the network" according to JCS, *Cyberspace Operations*, I-3.
10. Intelligence and National Security Alliance (INSA), Cyber Intelligence Task Force, *Operational Levels of Cyber Intelligence* (Arlington, VA: INSA, 2013), 1.
11. *Worldwide Threats to the Homeland, Hearing Before the Senate Committee on Homeland Security* (17 September 2014) (statement of Matthew G. Olsen, director National Counterterrorism Center).
12. Elias Groll, "Welcome to the Future of War: ISIS Has a Smartphone App," *Foreign Policy*, 8

December 2015, http://foreignpolicy.com/2015/12/08/welcome-to-the-future-of-war-isis-has-a-smartphone-app/.

13. National Intelligence Council (NIC), *Global Trends 2030: Alternative Worlds* (Washington, DC: NIC, 2012), 86.
14. Marc Lynch, Deen Freelon, and Sean Aday, "Blogs and Bullets III: Syria's Socially Mediated Civil War," *Peaceworks*, no. 91 (2014), www.usip.org/sites/default/files/PW91-Syrias%20Socially%20Mediated%20Civil%20War.pdf.
15. J. M. Berger and Jonathon Morgan, *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*, Brookings Project on U.S. Relations with the Islamic World, Analysis Paper No. 20 (Washington, DC: Brookings, 2015), 2; and Brian Bennett, "With Islamic State Using Instant Messaging Apps, FBI Seeks Access to Data," *Los Angeles Times*, 8 June 2015, www.latimes.com/world/middleeast/la-fg-terror-messaging-20150608-story.html#page=1 1/5.
16. Gabriel Weimann, *New Terrorism and New Media* (Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars, 2014), 2; and Haroro J. Ingram, "Three Traits of the Islamic State's Information Warfare," *RUSI Journal* 159, no. 6 (2004): 4–11, doi:10.1080/03071847.2014.990810.
17. Eric Liu, *Al Qaeda Electronic: A Sleeping Dog?* (Washington, DC: American Enterprise Institute Critical Threats Project, 2015), http://www.criticalthreats.org/sites/default/files/Al_Qaeda_Electronic.pdf.
18. Joseph A. Carter, Shiraz Maher, and Peter R. Neumann, *#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks* (London: International Centre for the Study of Radicalisation and Political Violence, 2014), www.icsr.info/wp-content/uploads/2014/04/ICSR-Report-Greenbirds-Measuring-Importance-and-Infleunce-in-Syrian-Foreign-Fighter-Networks.pdf.
19. Robert Hannigan, "The Web Is a Terrorist's Command-and-Control Network of Choice," *Financial Times*, 3 November 2014, http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3yXscPso1.
20. Bruce Schneier, "Hacker or Spy? In Today's Cyberattacks, Finding the Culprit Is a Troubling Puzzle," *Christian Science Monitor*, 4 March 2015, www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0304/Hacker-or-spy-In-today-s-cyberattacks-finding-the-culprit-is-a-troubling-puzzle.
21. Ibid.
22. Weimann, *New Terrorism and New Media*, 1.
23. Ibid., 10.
24. Brian Bennett, David S. Cloud, and W. J. Hennigan, "Pentagon Weighs Cybercampaign against Islamic State," *Los Angeles Times*, 20 December 2015, http://www.latimes.com/world/la-fg-cyber-isis-20151220-story.html.
25. Scott Shane, Matt Apuzzo, and Eric Schmitt, "Americans Attracted to ISIS Find an 'Echo Chamber' on Social Media," *New York Times*, 8 December 2015, http://nyti.ms/1NKAFzy.
26. Bennett, "With Islamic State Using Instant Messaging Apps."
27. "Islamic State Unfriended," *Economist*, 12 December 2015, http://www.economist.com/node/21679805/print.
28. "Tor was originally designed, implemented, and deployed as a third-generation onion routing project of the Naval Research Laboratory. It was originally developed with the U.S. Navy in mind, for the primary purpose of protecting government communications. Today, it is used every day for a wide variety of purposes by the military, journalists, law enforcement officers, activists, and many others." See "Inception," Tor, 28 January 2016, https://www.torproject.org/about/torusers.html.en. For one recent overview on the national security implications, see Eric Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing*, Global Commission on Internet Governance Paper Series 21 (Waterloo, ON, Canada: Centre for International Governance Innovation, London: Chatham House, 2015).
29. Michael Chertoff and Tobby Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security*, Global Commission on Internet Governance Paper Series No. 6 (Waterloo, ON, Canada: Centre for International Governance Innovation, London: Chat-

ham House, 2015), 1, https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.

30. For a discussion of the potential for anonymous use of Bitcoin, see Edward V. Murphy, M. Maureen Murphy, and Michael V. Seitzinger, *Bitcoin: Questions, Answers, and Analysis of Legal Issues* (Washington, DC: Congressional Research Service, 2015), 3.
31. Although Bitcoin does not reveal the user's actual identity, the record of transactions is completely public in the form of a block chain that could be used in some instances to infer identity. For a discussion, see Joshua Baron et al., *National Security Implications of Virtual Currency: Examining the Potential for Non-state Actor Deployment* (Santa Monica, CA: Rand, 2015).
32. Aaron Brantly, "Financing Terror Bit by Bit," *CTC Sentinel* 7, no. 10 (October 2014): 1–5.
33. Tim Fernholz, "Terrorism Finance Trackers Worry ISIS Already Using Bitcoin," *Defense One*, 13 February 2015, www.defenseone.com/threats/2015/02/terrorism-finance-trackers-worry-isis-already-using-bitcoin/105345/?oref=defenseone_today_nl.
34. Patrick Tucker, "How the Military Will Fight ISIS on the Dark Web," *Defense One*, 24 February 2015, www.defenseone.com/technology/2015/02/how-military-will-fight-isis-dark-web/105948/?oref=defenseone_today_nl.
35. Doug Bernard, "Crime and Espionage Becoming Tangled Online," *Voice of America*, 5 September 2015, http://www.voanews.com/content/crime-and-espionage-becoming-tangled-online/2949167.html.
36. Ibid.
37. Edwin Grohe, "The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict," *Comparative Strategy* 34, no. 2 (2015): 133–48, doi:10.1080/01495933.2015.1017342.
38. Daniel Regalado, Nart Villeneuve, and John Scott Railton, *Behind the Syrian Conflict's Digital Front Lines* (Milpitas, CA: FireEye, 2015), 5.
39. Ibid., 18.
40. Grohe, "The Cyber Dimensions of the Syrian Civil War," 140.
41. David E. Sanger and Eric Schmitt, "Hackers Use Old Lure on Web to Help Syrian Government," *New York Times*, 1 February 2015, www.nytimes.com/2015/02/02/world/middleeast/hackers-use-old-web-lure-to-aid-assad.html?_r=0.
42. Robert A. Johnson, "Predicting Future War," *Parameters* 44, no. 1 (Spring 2014).
43. JCS, *Joint Operations*, JP 3-0 (Washington, DC: DOD, 2011), GL-8, defines *cyberspace* operations as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." DOD, Office of the General Counsel, *Law of War Manual* (Washington, DC: DOD, June 2015), para. 16.1.2, states that "cyber operations: (1) use cyber capabilities, such as computers, software tools, or networks; and (2) have a primary purpose of achieving objectives or effects in or through cyberspace." This second tenet presents the ambiguity for the described situations above because many of the intended effects are for the ground or physical battlespace, rather than cyberspace.
44. Erick Waage, "Phreaker, Maker, Hacker, Ranger: One Vision for Cyber Support to Corps and Below in 2025," *Small Wars Journal* (blog), 11 August 2015, http://smallwarsjournal.com/jrnl/art/phreaker-maker-hacker-ranger-onevision-for-cyber-support-to-corps-and-below-in-2025.
45. DOD, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: DOD, 2011), http://www.defense.gov/news/d20110714cyber.pdf.
46. This viewpoint is implicitly articulated in the establishment of U.S. Cyber Command as a subunified command of U.S. Strategic Command, responsible for coordinating the cyberactivities of the individual military Services. *Department of Defense Strategy for Operating in Cyberspace* specifically states on page 5 that "DoD will organize, train, and equip for the complex challenges and vast opportunities of cyberspace."
47. Catherine Lotrionte, "Statecraft in Cyberspace," *Cipher Brief*, 13 December 2015, https://www.thecipherbrief.com/article/statecraft-cyberspace.
48. William J. Lynn III, ed., "Defending a New Domain: The Pentagon's Cyberstrategy," *Council on Foreign Relations*, September/October 2010, https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain?gp=66687%3A31ac65264c9a4440.
49. JCS, *Joint Targeting*, C-7.

50. Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1 (2014): 9, doi:10.1080/01402390.2014.977382.
51. The Army and other Services have recognized these shortfalls and prioritized establishment of capabilities at this level. One means to do so is developing cyberteams that can find, fix, and mitigate currently undetected malicious actors in military networks and provide capabilities to integrate cyberexpertise into Army land operations to support tactical and operational cyberplanning and integration. See, Jeffrey L. Caton, *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications* (Carlisle Barracks, PA: U.S. Army War College Press, 2015), http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1246.pdf.
52. JCS, *Cyberspace Operations*, I-2.
53. Paul Roderick Gregory, "Putin's New Weapon in the Ukraine Propaganda War: Internet Trolls," *Forbes*, 9 December 2014, http://www.forbes.com/sites/paulroderickgregory/2014/12/09/putins-new-weapon-in-the-ukraine-propaganda-war-internet-trolls/.
54. For a discussion on this point and cybertargeting methodology, in general, see Robert Fanelli and Gregory Conti, "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict," in *2012 4th International Conference on Cyber Conflict*, ed. C. Czosseck, R. Ottis, and K. Ziolkowski (Tallinn, Estonia: North Atlantic Treaty Organization Cooperative Cyber Defence Center of Excellence, 2012).
55. DOD, *The Department of Defense Cyber Strategy* (Washington, DC: DOD, 2015), 12, www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
56. Cyber Intelligence Task Force, *Operational Levels of Cyber Intelligence*, 11.
57. Ibid.
58. DOD, *Department of Defense Cyber Strategy*, 11.
59. Patrick Tucker, " 'Jihadi John' and the Future of the Biometrics Terror Hunt," *Defense One*, 27 February 2015, http://www.defenseone.com/technology/2015/02/jihadi-john-and-future-biometrics-terror-hunt/106263/.
60. Liang Wang and Xin Geng, *Behavioral Biometrics for Human Identification: Intelligent Applications* (Hershey, PA: Medical Information Science Reference, 2010), 26.
61. Roman V. Yampolskiy and Venu Govindaraju, "Behavioural Biometrics: A Survey and Classification," *International Journal of Biometrics* 1, no. 1 (2008): 81–113.
62. For one recent example of these applications, see patent filing for Israeli behavioral biometrics firm BioCatch and the related article, Stephen Mayhew, "BioCatch Granted Behavioural Biometric Patent for Mobiles," Planet Biometrics, 24 February 2015, www.planetbiometrics.com/article-details/i/2746.
63. James Vincent, "Behaviosec Uses 'Behavioral Biometrics' to Find if the Person Using a Mobile Device Is Really Who They Claim to Be," *Economic Times*, 2 September 2014, www.economictimes.indiatimes.com/news/international/business/behaviosec-uses-behavioural-biometrics-to-find-if-the-person-using-a-mobile-device-is-really-who-they-claim-to-be/articleshow/41463585.cms.
64. Yedid Hoshen and Shmuel Peleg, "Egocentric Video Biometrics," Hebrew University of Jerusalem, 27 November 2014, www.arxiv.org/pdf/1411.7591v1.pdf.
65. Julian E. Barnes, "U.S. Military Plugs into Social Media for Intelligence Gathering: Defense Intelligence Agency Head Says Online Postings Played Crucial Role in Ukraine Jet Shootdown Investigation," *Wall Street Journal*, 6 August 2014, http://www.wsj.com/articles/u-s-military-plugs-into-social-media-for-intelligence-gathering-1407346557.
66. Babak Hodjat, "Myth Busting Artificial Intelligence," *Wired Magazine*, http://www.wired.com/insights/2015/02/myth-busting-artificial-intelligence/.
67. Quentin Hardy, "Facebook Offers Artificial Intelligence Tech to Open Source Group," *New York Times Bits* (blog), 16 January 2015, http://bits.blogs.nytimes.com/2015/01/16/facebook-offers-artificial-intelligence-tech-to-open-source-group/.
68. Gabriel Miller, "Activity-Based Intelligence Uses Metadata to Map Adversary Networks," *Defense News*, 8 July 2013.
69. For a useful, recent introduction, see Paul B. Symon and Arzan Tarapore, "Defense

Intelligence Analysis in the Age of Big Data," *Joint Forces Quarterly*, no. 79 (4th Quarter 2015): 4–11, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_4-11_Symon-Tarapore.pdf.

70. Chandler P. Atwood, "Activity-Based Intelligence: Revolutionizing Military Intelligence Analysis," *Joint Forces Quarterly*, no. 77 (2d Quarter 2015): 24–33, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_24-33_Atwood.pdf.
71. Mark Phillips, "A Brief Overview of ABI and Human Domain Analytics," *Trajectory Magazine*, 2012, http://trajectorymagazine.com/civil/item/1369-human-domain-analytics.html.
72. Catherine Johnston et al., "Transforming Defense Analysis," *Joint Forces Quarterly*, no. 79 (4th Quarter 2015): 12–18, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_12-18_Johnston-et-al.pdf.
73. Shawn Riley, *Science of Cybersecurity: Developing Scientific Foundations for the Operational Cybersecurity Ecosystem* (Washington, DC: Centre for Strategic Cyberspace + Security Science), 11 August 2015, http://cscss.org/wp-content/uploads/2015/08/CSCSS-Science-of-Security-Developing-Scientific-Foundations-for-the-Operational-Cybersecurity-Ecosystem.pdf.
74. Adam Tanner, "How Ads Follow You from Phone to Desktop to Tablet," *MIT Technology Review*, 1 July 2015, www.technologyreview.com/news/538731/how-ads-follow-you-from-phone-to-desktop-to-tablet/.
75. NIC, *Global Trends 2030*, 88.